Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report for 01 July 2004

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

Daily Overview

- CNET News reports that a malicious program that installs itself through a pop−up can read keystrokes and steal passwords when victims visit any of nearly 50 targeted banking sites. (See item 9)
- Bloomberg reports the European Commission has proposed widening the net to catch money launderers and terrorists with new transaction reporting duties for attorneys, insurance brokers and other businesses beyond the banking system. (See item 10)
- The Arkansas News Bureau reports that Arkansas has set new reporting requirements for several communicable diseases because of their potential connection to bioterrorism. (See item 27)
- The Department of Homeland Security reports the Federal Emergency Management Agency has announced a new online course that will help first responders understand the concepts and principles underlying the new National Incident Management System. (See item 34)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *June 30, Agence France−Presse* — **U.S. crude oil inventories slip, survey shows. U.S. commercial inventories of crude oil slipped last week and stocks of gasoline were flat, a**

survey by the Department of Energy showed. A separate survey by the private American Petroleum Institute (API) also showed a decline in commercial crude oil stocks but it found gasoline stocks fell in the same period. **According to the government, crude oil stocks dropped 500,000 barrels to 304.9 million in the week to June 25 when compared to the previous week.** The Department of Energy said gasoline stocks were flat at 205.1 million barrels. Distillates −− diesel and heating oil −− rose 500,000 barrels to 110.9 million, it said. The API found inventories of crude oil dropped 4.2 million barrels to 304.6 million, gasoline fell 2.1 million barrels to 204.1 million and distillates declined 1.6 million to 110.9 million.
Source: http://news.yahoo.com/news?tmpl=story&u=/afp/20040630/ts_afp/us_oil_inventories_040630192200

2. *June 30, Reuters* — **U.S. sees higher OPEC output despite lower oil price. The Organization of Petroleum Exporting Countries (OPEC) needs to stick to its pledge to raise crude oil output by 500,000 barrels per day on August 1, even though U.S. oil prices are lower and inventories are higher, U.S. Secretary of Energy Spencer Abraham said** on Wednesday, June 30. "Clearly the demand (for oil) has not abated ... I hope they (OPEC member countries) will fulfill the commitments they've made," Abraham said. To help lower global oil prices and meet demand, OPEC is raising its oil output by 2 million bpd, effective July 1, from 23.5 million, with another 500,000 bpd increase due in August. It meets on July 21 to review the second stage of the increase. "There is greater (oil) production than a year ago, and we have more inventory than we do a year ago, but the world is demanding more," Abraham said. **OPEC provides about half of global oil trade. Oil use in 2004 is expected to grow at 2.9 percent, the fastest rate in 23 years, according to the International Energy Agency.**
Source: http://www.washingtonpost.com/wp−dyn/articles/A18274−2004Jun 30.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

3. *June 30, Associated Press* — **Explosive chemical forces evacuation at university. The discovery of a chemical that had solidified with age into a potential explosive forced an evacuation at Clark Atlanta University for about two hours Tuesday, June 29, until the substance could be neutralized.** About 200 students and faculty members were affected by the evacuation after a cleaning crew found several 2 1/2− to 5−pound containers of dried picric acid at the school's science center about 2:30 p.m. A private contracting crew arrived about 4 p.m. to render the chemical safe, and students were allowed back into the science center and surrounding buildings about 5 p.m., Atlanta Fire Department spokesperson Jolene Butts Freeman said. Freeman said that when picric acid solidifies it can be equivalent to dynamite. She did not know how long the acid had been stored there.
Source: http://www.macon.com/mld/macon/news/politics/9041790.htm

4. *June 30, Agence Presse−France* — **Pollution scare as acid ship sinks in German port. A German ship with carrying nearly 1000 tons of sulphuric acid has sunk in the German port of Hamburg, raising fears of a major environmental accident. The vessel, the ENA−2, went down on Monday evening, June 28, after hitting a container vessel, firefighters said on Tuesday.** Nine port employees and two police officers were taken to

hospital with breathing difficulties after inhaling gas from the ship's ventilation system. The authorities said there was still a risk of a major leak during operations to re−float the 62−metre (200−foot) ship. "Re−floating will not begin until Wednesday. It is going to be a delicate operation," a firefighters spokesman said, adding that if the ship broke up conditions would be "perfect for an ecological catastrophe." **Experts said a disaster would have been inevitable had the double hull structure of the ship been damaged when it struck the container ship during docking procedures.** Reports that the captain of the German−registered chemical carrier had been drunk during docking were being investigated. The ENA−2, owned by Norddeutsche Affinerie (NA), had been maneuvering into the Hamburg oil terminal when it hit with the container vessel. The tanker managed to dock, but then sank at its moorings.
Source: http://www.terradaily.com/2004/040629145546.o4gaskmo.html

5. *June 30, Associated Press* — **Ammonia leak causes evacuation of residents. Residents within a one−mile radius of an old mine site in Preston County, WV, were asked to leave their homes Tuesday, June 29, after an ammonia leak.** No injuries were reported, but emergency officials ordered evacuations because vapors from anhydrous ammonia can irritate the eyes and respiratory tract. The chemical, which is used to treat acid mine drainage, can be fatal if inhaled in large doses. The leak occurred at the Squire's Creek Mine when a valve on a storage tank failed. **Officials with the state Department of Environmental Protection said about 6,000 gallons of ammonia turned to gas and produced a chemical cloud.** Patriot Mining Company Inc., a subsidiary of Anker Coal Co., owns the inactive mine. Though the ammonia is stored in a 12,000−gallon tank, Environmental Protection Agency records available online indicate the tank is never filled more than 85 percent. EPA records indicate there have been no accidents at the site in the past five years. Patriot employees are trained in the safe handling, storage and use of anhydrous ammonia, as well as what to do if there is an accidental release.
Source: http://www.herald−mail.com/?module=displaystory&story_id=823 53&format=html

[Return to top]

Defense Industrial Base Sector

6. *June 29, Govexec.com* — **State, local officials lukewarm on base−closing delay. Several lawmakers are fighting to delay next year's scheduled round of military base closings for two years, but many state and local leaders in areas with military installations are less than enthusiastic about the idea.** Bob Johnstone, executive director of the Southwestern Defense Alliance, which hopes to preserve research, test and training ranges in seven southwestern states and California, says there's never a good time for base closures. But, he adds, "most communities I have talked to are opposed [to a delay]. They want to get it over with and quit wasting money on lobbyists." Adrian King, deputy chief of staff for Pennsylvania Governor Edward Rendell, says his state is "on the fence" about backing a delay. **King says having a guarantee that the state would not lose jobs at its bases for two more years is attractive, but he adds that Pennsylvania could gain work in the process of transforming bases and would welcome those jobs as soon as possible.** Secretary of Defense Donald Rumsfeld has said that the military wastes billion of dollars annually maintaining as much as 25 percent excess base infrastructure. Congress has been split on the issue.
Source: http://www.govexec.com/dailyfed/0604/062904g1.htm

7. *June 29, Govexec.com* — **Army to seek waiver of limits on contracting repair work.** As the Army continues extensive operations in Iraq and Afghanistan, service leaders are seeking a waiver to hire more contractors to repair worn−out equipment. **Lt. Gen. Claude Christianson, the Army's deputy chief of staff for logistics, said on Tuesday, June 29, that the service will ask Congress to waive a federal law requiring that half of all work at military repair and maintenance depots be performed by federal workers. He said the waiver is necessary because weapons systems, particularly Army helicopters, are wearing out at far greater rates than planned.** Christianson said the Army likely will only need to breach the 50−50 threshold at the Corpus Christi Army Depot in Texas, where helicopters are repaired. However, he said the service will request the waiver for its other four depots as well. Those depots repair Army tracked and ground vehicles and communications systems. Congress passed the 50−50 law to limit outsourcing of repair work, which is done by thousands of Department of Defense civilian workers. The Army expects to increase spending and production at depots this year by 25 percent.
   Source: http://www.govexec.com/dailyfed/0604/062904g2.htm

[Return to top]

Banking and Finance Sector

8. *June 30, ComputerWeekly* — **Banks, brokerages dogged by e−mail regulations.** IT managers in the financial services industry are finding it increasingly difficult to comply with regulations that force banks and brokerages to store and be able to easily access e−mail and instant messaging (IM) exchanges with customers. Several financial regulatory agencies have recently imposed regulations about the type of information broker/dealers can share with clients via e−mail or IM −− as well as how long those messages must be stored so they can be retrieved for audit. Brokerages frequently automate and test backup and recovery of e−mail and IM, but those efforts are probably not done "consistently enough to meet regulatory requirements," said Andy Welch, a senior manager for KPMG. One of the key challenges that securities firms face is being able to retrieve and present customer e−mail correspondence to regulators within 24 hours, as required under some regulations. **Regulators at the Federal Deposit Insurance Company (FDIC) are also concerned about the potential network vulnerabilities created when bank employees use IM. Attempts by banks to secure IM exchanges using a firewall have so far proved difficult,** said Kathryn Weatherby, an examination specialist in the FDIC's division of supervision and consumer protection.
   Source: http://www.computerweekly.com/articles/article.asp?liArticleID=131646&liFlavourID=1&sp=1

9. *June 30, CNET News* — **Renegade program stealing passwords at banking sites. A malicious program that installs itself through a pop−up can read keystrokes and steal passwords when victims visit any of nearly 50 targeted banking sites, security researchers warned** Tuesday, June 29. The targeted sites include major financial institutions, such as Citibank, Barclays Bank and Deutsche Bank, researcher Marcus Sachs said. "If [the program] recognizes that you are on one of those sites, it does keystroke logging," said Sachs, director of the Internet Storm Center, a site that monitors network threats. **Even though all financial sites use encryption built into the browser to protect log−in data, the Trojan horse program**

can capture the information before it gets encrypted by the browser software. Researchers at the Internet Storm Center studied the Trojan horse file, called "img1big.gif." The program points to a recent trend in computer viruses and remote−access Trojan horse, or RAT, programs: attackers are increasingly after money. Because it carries a .gif file extension, the Trojan horse appears to be a graphic in a compressed format commonly found on the Internet. In reality, it's two programs: a browser helper file that surreptitiously captures usernames and passwords, and a "file dropper" that installs the keyword logger on the victim's computer.
Source: http://www.silicon.com/0,39024729,39121778,00.htm

10. *June 30, Bloomberg* — **EU expands financial reporting to catch money laundering, terrorism funding.** The European Commission proposed widening the net to catch money launderers and terrorists with new transaction reporting duties for attorneys, insurance brokers and other businesses beyond the banking system. **The European Union's (EU) executive arm in Brussels, Belgium, is seeking to require that businesses verify customer identities, watch for suspicious transaction patterns and report any cash purchase of more than 15,000 euros (US$18,000). The rules would cover businesses such as service providers, trusts, jewelers, auction houses and casinos in the 25 EU countries, officials said.** The proposal aims to apply suggestions made last year by the Financial Action Task Force, a group of national law enforcement agencies and experts that meet under auspices of the Organization for Economic Cooperation and Development. The draft must be approved by EU governments and the European Parliament and then implemented by each member state. The proposal would be the EU's third set of rules on money laundering. The first was a 1991 directive aimed at drug dealers. The laws were broadened with a second directive after the 2001 terrorist attacks, which implied rather than specified terrorism as a target.
Source: http://quote.bloomberg.com/apps/news?pid=10000085&sid=api56WqXLkSs&refer=europe

11. *June 30, CNN/Money* — **New $50 bill debut set. The new multi−colored $50 bill will be released September 28, the Federal Reserve announced** Wednesday, June 30. The new bill has subtle background colors of blue and red, and images of a waving American flag and a small metallic silver−blue star. The new bills will be distributed through commercial banks starting on the release date. It will be the second bill to have colors other than green, following the new $20 bill, which started circulating last October. The new bills are meant to make counterfeiting more difficult. **Although the new colors are the most readily visible difference between the new and old bills, the new designs incorporate other anti−counterfeiting features. These include an embedded plastic strip, a watermark image engrained into the paper itself, and color−shifting ink, whose appearance changes as you tilt the bill against the light.** The Bureau of Engraving and Printing said Wednesday's announcement comes about 90 days before the September 28 rollout, giving makers of ATMs and other machines time to adjust to the new bill. Eventually, all currency is expected to be redesigned with new color schemes and anti−counterfeiting features.
Source: http://money.cnn.com/2004/06/30/news/economy/new_fifty/index .htm?cnn=yes

[Return to top]

Transportation Sector

12. *June 30, PR Newswire* — **Air Marshals should remain undercover.** The Association of Flight Attendants−CWA (AFA) today voiced its opposition to a scheme forcing federal air marshals to dress like stereotypical federal agents, warning that the policy jeopardizes the lives of airline passengers and crew. **The Federal Air Marshal Service has prohibited the use of less than formal attire and grooming, such as jeans, tattoos, long hair, and beards, even though such appearance would help the marshals blend in as ordinary passengers.** Instead, they must wear suits and ties, shiny shoes and short hair. Initially, they were permitted to make their own dress and grooming decisions. In April, the Federal Law Enforcement Officers Association (FLEOA) urged members of Congress to intervene. "The current dress code and military grooming policy compromise air marshals' identities, thus gravely jeopardizing aviation security. Easy identification of air marshals permit terrorists to distinguish between flights air marshals will be protecting, and more importantly, flights they won't be protecting. Source: http://www.afanet.org/afa/default.asp

13. *June 30, General Accounting Office* — **GAO−04−838: Maritime Security: Substantial Work Remains to Translate New Planning Requirements into Effective Port Security (Report).** The Maritime Transportation Security Act of 2002, as implemented by the Coast Guard, calls for owners and operators of about 3,150 port facilities (such as shipping terminals or factories with hazardous materials) and about 9,200 vessels (such as cargo ships, ferries, and tugs and barges) to develop and implement security plans by July 1, 2004. The Coast Guard intends to conduct on−site compliance inspections of all facilities by January 1, 2005, and all vessels by July 1, 2005, to ensure plans are adequately implemented. The General Accounting Office (GAO) was asked to assess (1) the progress towards developing, reviewing, and approving plans by July 1, 2004, (2) the Coast Guard's monitoring and oversight strategy for ensuring that plans are implemented, and (3) the accuracy of the Coast Guard's cost estimate. **GAO recommends that the Coast Guard evaluate its initial compliance efforts and use them to strengthen the compliance process for its long−term strategy. As part of this strategy, the Coast Guard should clearly define inspector qualifications and consider including unscheduled and unannounced inspections and covert testing**. The Coast Guard agreed. Highlights: http://www.gao.gov/highlights/d04838high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−04−838

14. *June 30, Richmond Times−Dispatch (VA)* — **Ferry service plans terror screening.** Special guards will start anti−terrorism screening on Virginia Department of Transportation's (VDOT) Jamestown−Scotland ferries Thursday, July 1. **The round−the−clock security planned for the James River ferry service is a portent of more such measures to protect public infrastructure in post−September 11 America, officials said**. VDOT is hiring contract security agents to run federally−required random screenings of passengers and their vehicles to prevent dangerous substances from getting on the ferries, the department said on June 29. "Anyone traveling the ferry is subject to screening," the state Transportation Department said. Guards may check driver and passenger identification and look under, around and into cars, trucks, campers and trailers, VDOT said. The security guards will be posted 24 hours a day at the old tollbooth locations on the river's Jamestown and Surry sides. Though the ferries will still depart on schedule, the highway agency warned, commuters should get ready for delays boarding the vessels once the screenings start, especially during times of higher alert. Four ferry boats −− the Pocahontas, the Williamsburg, the Surry, and the Virginia −− carry about 3,000 cars, trucks and tour buses a day during the tourist season and about 2,500 a day in the winter,

according to VDOT.
Source: http://www.timesdispatch.com/servlet/Satellite?pagename=RTD%2FMGArticle%2FRTD_BasicArticle&c=MGArticle&cid=1031776322853&path=!news&s=1045855934842

15. *June 30, Department of Transportation* — **FRA proposes to improve crash survivability of locomotive black box. Event recorders, the train equivalent of an airplane's "black box," will be improved to make sure critical information survives train accidents according to a proposed rule issued on June 30 by the Federal Railroad Administration (FRA).** "The survival of data is key to understanding why a train accident happened," said FRA Acting Administrator Betty Monro. The regulations proposed on June 30 are intended to prevent the loss of data resulting from train accidents involving fire, water, and significant mechanical damage. FRA also is proposing that improved event recorders collect and store additional data, including emergency braking systems, locomotive horns and text messages sent to the engineer's display regarding directives and authorized speed. The proposed rule would also simplify existing standards for inspecting, testing, and maintaining event recorders by railroads. The proposed regulations are based upon recommendations of the Railroad Safety Advisory Committee, a consensus−based rulemaking body comprised of representatives of railroads, industry labor organizations, manufacturers, suppliers and others.
Source: http://www.dot.gov/affairs/fra1004.htm

16. *June 29, Omaha World−Herald (NE)* — **Iowa to check for radioactive cargo.** Drive−through radiation detection equipment will be installed at five weigh stations on Interstates 35 and 80 later this year to look for radioactive cargo in heavy trucks. **State officials told the Des Moines Register that Iowa will become one of the first states in the country to routinely check trucks for the illegal cargo, as part of an effort to stop terrorists from smuggling bomb−making materials or stolen nuclear weapons**. Concerns over terrorists smuggling nuclear weapons or bomb−making materials have increased since the terror attacks of September 11, 2001, according to experts. A potential threat are the so−called dirty bombs that combine a conventional explosive such as dynamite with radioactive material that could be dispersed in an explosion. "Weigh stations are good places to detect the shipment of materials that can be used for weapons of mass destruction," said David Miller, chief of staff at the Iowa Division of Homeland Security and Emergency Management. Acquiring radiation detection equipment is part of the state's strategy to combat terrorism, Miller said. Law enforcement officers who work at the weigh stations will be given hand−held devices that can check for explosives.
Source: http://www.omaha.com/index.php?u_np=0&u_pg=1638&u_sid=113504 1

17. *June 29, PR Newswire* — **Members of the ICCL fully compliant with ISPS Code.** The International Council of Cruise Lines (ICCL) announced June 29, 2004, that all 118 vessels of its member lines are 100% compliant with the International Ship and Port Facility Security (ISPS) Code. This announcement comes two days before the July 1 deadline for all ships and port facilities worldwide. **The ISPS Code is a set of measures that enhance security of ships and port facilities globally, adopted by the International Maritime Organization (IMO) as an amendment to Safety of Life at Sea (SOLAS) regulations**. Key security elements contained in the ISPS Code include security plans, screening measures, access control, waterside security and communications between ships and ports. "ICCL applauds our members

for their responsiveness to the ISPS deadline," said Michael Crye, president of ICCL.
Source: http://www.iccl.org/pressroom/pressrelease.cfm?whichrel=43

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

18. *June 30, Food Navigator* — **Scientist calls for risk test to protect chocolate crops.** A persistent threat to the chocolate industry witches' broom disease (WBD) is capable of wiping out entire cocao crops. Despite ongoing research into the threat, a UK scientist warns this week that more needs to be done to assess the risk of this fungal disease. In the 1990s WBD, ripped its way through the main Brazilian cocoa region of Bahia, leaving 200,000 without work and decimating cacao supplies. As a result, in 10 years Brazil has gone from being the world's second−largest exporter of cocoa beans to a net importer. **Research programs including an attempt to sequence the genes of the pathogen, are aiming to shed light on this difficult disease that is proving extremely tricky to solve.** But according to Gareth Griffith, a plant pathologist at the University of Wales, a risk assessment should be carried out as soon as possible. **Griffith is calling for immediate research to quantify the risk of WBD spreading to West Africa, an assessment that could be quickly carried out with immediate benefits.** West Africa now accounts for 70 percent of the world's output of cocoa beans.
Source: http://www.foodnavigator.com/news/news−NG.asp?id=53177

19. *June 30, Xinhuanet* — **Bird flu kills chickens in Vietnam. Bird flu has recurred in Vietnam, killing about 5,000 fowls in the country's southern Bac Lieu province, a local official told Xinhua on Wednesday, June 30.** "Tests conducted in the regional veterinary center in Ho Chi Minh City have confirmed that all of the fowls were tested positive for an H5 strain of bird flu," said Nguyen Phuc Tai, director of the veterinary department of Bac Lieu province. The fowls from two farms and a household have suddenly died since June 25, he said, adding that the province has culled all of the infected fowls in an effort to contain the virus. Reasons for the bird flu's return in the locality have been studied, Tai said.
Source: http://news.xinhuanet.com/english/2004−06/30/content_1557544 .htm

20. *June 30, PR Newswire* — **DuPont acquires BioSentry's animal health business assets. DuPont announced it has acquired the animal health business assets of BioSentry Inc., a leading biosecurity company providing animal health prevention programs in 50 countries.** Financial terms were not disclosed. The acquisition furthers DuPont's strategy and positioning as a global leader in the safety and protection industry. BioSentry, which has biosecurity sales in 50 countries, has been in the forefront of animal health and hygiene for nearly 50 years. Based in Atlanta, GA, the company offers a comprehensive biosecurity program, including an integrated line of innovative clean and disinfectant products that are tailored to address specific needs in animal and food safety. BioSentry will be integrated into

the DuPont Chemical Solutions Enterprise business, which is part of the DuPont Safety & Protection (DSP) growth platform.
Source: http://www.prnewswire.com/cgi−bin/stories.pl?ACCT=109&STORY=/www/story/06−30−2004/0002202690&EDATE=

21. *June 29, Columbus Telegram (NE)* — **Group to buy Furnas Farms. A group of Nebraska livestock producers has won the right to purchase Columbus, NE, based Furnas County Farms for about $57 million.** Furnas lawyer Joseph Badami confirmed the sale, which is subject to approval by the bankruptcy court. The offer was made by Nebraska Pork Partners, a general partnership "led by individuals who are Nebraska livestock producers," according to a press release by Ag and Food Associates, which managed the offer. The release did not say who makes up Nebraska Pork Partners. The release said the group plans to keep the operation running and will keep its headquarters in Columbus "for the foreseeable future." Furnas employs 375 people, mostly in Nebraska, at 80 sites and has an average annual payroll totaling more than $8 million, according to court records. At any one time, Furnas is responsible for feeding and marketing 430,000 hogs −− about 15 percent of all hogs in Nebraska.
Source: http://www.columbustelegram.com/articles/2004/06/29/news/new s3.txt

[Return to top]

Food Sector

22. *June 30, USAgNet* — **USDA awaits results of more mad cow tests.** The U.S. Department of Agriculture (USDA) and the beef industry are awaiting additional tests to determine whether two animals singled out in preliminary screening had mad cow disease. **The USDA on Tuesday, June 29, announced an "inconclusive" test result on a second animal, indicating the possible presence of the disease. It was the second such discovery in five days as part of the government's rapid screening program.** Officials pointed out that the initial test is so sensitive it does not mean new cases have been found. The only confirmed U.S. case of mad cow was discovered in Washington state last December, prompting more sophisticated screening for the disease. Tissue samples from the animals discovered Friday, June 25, and Tuesday, June 28, were being examined at the USDA's National Veterinary Services Laboratories.
Source: http://www.usagnet.com/story−national.cfm?Id=682&yr=2004

23. *June 29, Food Safety and Inspection Service* — **Beef jerky recall. Hockenberry Processing, a Fort Loudon, PA, firm is voluntarily recalling approximately 130 pounds of beef jerky that may be contaminated with Listeria monocytogenes, the U.S. Food Safety and Inspection Service (FSIS) announced Tuesday, June 29.** The recalled products were produced on June 10 and June 11, 2004 and shipped to retail distributors in New York and Pennsylvania. The problem was discovered by the company. FSIS has received no reports of illnesses associated with consumption of this product. Consumption of food contaminated with Listeria monocytogenes can cause listeriosis, an uncommon but potentially fatal disease. Healthy people rarely contract listeriosis. However, listeriosis can cause high fever, severe headache, neck stiffness, and nausea. Listeriosis can also cause miscarriages and stillbirths, as well as serious and sometimes fatal infections in those with weak immune systems.
Source: http://www.fsis.usda.gov/News_&_Events/Recall_022_2004_Relea se/index.asp

[Return to top]

Water Sector

24. *June 30, Salinas Californian* — **Prison's water supply tainted. Inmates' drinking water has been rationed at Salinas Valley State Prison (SVSP) and showering and toilet flushing curtailed since late last week, when nitrate contamination was confirmed in the only well serving the prison.** The California Department of Health Services confirmed Tuesday, June 29, that the only well on the premises of SVSP in Soledad has tested over the acceptable limit for nitrate, a contaminant found in fertilizer and in human and animal waste. No inmates or staff members or nearby residents are at risk from the contaminated water, prison officials said. Since Friday, June 25, the prison has augmented its water supply by mixing stored, uncontaminated water with water imported from the Correctional Training Facility nearby.
Source: http://www.californianonline.com/news/stories/20040630/local news/748660.html

25. *June 30, BBC News* — **Scientists make arsenic water link. Scientists in the United Kingdom say they have made a significant step forward in understanding why drinking water in Bangladesh and the Indian state of West Bengal is contaminated with arsenic. The researchers say their finding may lead to new ways of eliminating it from drinking water.** The arsenic crisis first came to light about 20 years ago. It is now estimated that tens of millions of people have been poisoned by drinking contaminated water from wells. Arsenic gets into the water deep underground, by natural processes which are poorly understood. Now researchers at Manchester University have shown that certain kinds of bacteria are involved, stripping arsenic from earth and depositing it in water which will later be drawn up in wells and drunk. "Now we understand a little bit more the processes that are taking place, we can for instance predict at−risk wells a little bit more accurately," says Jonathan Lloyd, the head of the research team. "Maybe we can come up with strategies for controlling the water flow a little better, to try and prevent these problems taking place."
Source: http://news.bbc.co.uk/2/hi/south_asia/3854709.stm

26. *June 30, Los Angeles Times* — **Water emergency declared in Wrightwood. The four−year drought that has heightened the fire danger in the San Bernardino Mountains and forced water restrictions on several mountain communities prompted county officials Tuesday, June 29, to declare an emergency water shortage in the resort town of Wrightwood, CA.** Water levels in underground wells and reservoirs in the mountains have dropped more than 20 percent in the past few weeks, forcing the San Bernardino County Board of Supervisors to adopt an emergency measure to haul county water by tanker truck to replenish a Wrightwood reservoir. Other mountain communities that rely solely on underground water sources have also imposed restrictions in response to the worsening drought. But county officials said Wrightwood's shortage is so severe that they feared firefighters would be unable to douse a blaze in the surrounding tinder−dry woods.
Source: http://ktla.trb.com/news/local/ktla−me−water30jun30−lat,0,6621499.story?coll=ktla−news−1

[Return to top]

Public Health Sector

27. *June 30, Arkansas News Bureau* — **Bioterrorism threat sparks new disease reporting. Arkansas has set new reporting requirements for several communicable diseases because of their potential connection to bioterrorism. The medical community must immediately report suspected or confirmed diagnosis of Anthrax, Botulism, Plague, Smallpox, Tularemia, and Viral Hemorrhagic Fevers.** Those diseases could be linked to bioterrorism, said Frank Wilson, state epidemiologist for the Health Department. "The biggest change in this is asking for immediate reporting of certain conditions −− that is day or night as soon as it is suspected, by telephone, which we have not asked for before," Wilson said. Immediate, 24−hour−a−day notice also is being required of suspected Hepatitis A, Meningococcal Infection, Pertussis, Q Fever, Severe Acute Respiratoey Syndrome (SARS), and Typhus. Those diseases aren't linked to bioterrorism, but Wilson said they merit immediate notice. The new rules became effective on Monday, June 28, after being approved in April by the state Board of Health. The expanded reporting is required of doctors, practitioners, nurses, superintendents in dispensaries, hospitals, clinics, nursing or extended care homes, and laboratory personnel examining human specimens resulting in the diagnosis of suspect or confirmed diseases, according to the Health Department.
Source: http://www.arkansasnews.com/archive/2004/06/30/News/247824.h tml

28. *June 30, United Press International* — **Accounting shift threatens vaccine program. Drug companies that have participated for decades in a federal program to stockpile children's vaccines are considering withdrawing because new accounting guidelines require them to delay booking production payments as revenue until the drugs are removed from the stockpiles for use.** The shift could mean a delay of up to a year in recognizing revenue from the contracts, potentially hurting officially reported profits and earnings per share and, by extension, stock prices. The problem is serious enough that Aventis, one of the world's largest vaccine manufacturers, already has told the U.S. Centers for Disease Control and Prevention (CDC) it will not extend a stockpile contract. CDC officials are worried other firms might back out as well. "It is definitely a concern," said Stephen Cochi, acting director of the CDC's National Immunization Program. The agency has maintained stockpiles of selected childhood vaccines since the 1980s. These caches enable public health officials to respond to sudden outbreaks of illness, bridge disruptions in supplies, and reduce the cost of vaccinations through negotiated purchases. The CDC recently tapped into the reserves to help the Marshall Islands deal with an outbreak of measles.
Source: http://www.upi.com/view.cfm?StoryID=20040629−063134−5244r

29. *June 30, Reuters* — **Pentagon expands anthrax, smallpox vaccinations. The Pentagon plans to expand the number of troops receiving anthrax and smallpox vaccinations to forces based in South Korea, officials said on Wednesday, June 30.** Deputy Defense Secretary Paul Wolfowitz, in a memo released on Wednesday, called the Pentagon's vaccination programs to protect troops against exposure to these germ warfare agents a success. "Building on that success and the continued threat of biological attack, it is prudent to expand our immunization programs now," Wolfowitz said in the memo. The memo said the expansion affected U.S. forces in South Korea and added to the numbers of troops deployed in the Middle East getting the shots.
Source: http://www.reuters.com/newsArticle.jhtml?type=topNews&storyI D=5554889

30. *June 30, University of Pennsylvania* — **Bacterial protein recycling factor possible key to new class of antibiotics.** Understanding the last step of protein synthesis −− the basic process of translating DNA into its final protein product −− just became more clear both literally and figuratively. This final phase, called recycling, is essential for the proper function of all cells. Using a three−dimensional cryo−electron microscope to directly observe protein structure, investigators at the University of Pennsylvania School of Medicine and the State University of New York, Albany can now visualize the exact configuration of a molecule called ribosome recycling factor (RRF) in the common bacteria Escherichia coli. **This image may help guide the design of new antibiotics aimed at inhibiting RRF−related steps of protein synthesis. Most antibiotics influencing protein synthesis act by stopping its molecular machinery. However, none as yet target the recycling step.**
Source: http://www.uphs.upenn.edu/news/News_Releases/june04/Bacteria lRRF.htm

[Return to top]

Government Sector

31. *June 29, Government Computer News* — **Information sharing networks overlap as policy gels.** Information sharing networks being developed by the Department of Homeland Security (DHS) and the law enforcement and intelligence communities are beginning to provide overlapping capabilities, especially at the secret level. **DHS officials speaking at the Information Sharing for Homeland Security symposium said they plan to expand the Homeland Security Information network (HSIN), launched in February, to the secret level by the end of this year.** The system now operates at the sensitive but unclassified level. Meanwhile, the intelligence community plans this year to expand the Terrorist Threat Integration Center (TTIC) Online network, now operating at the top secret level, to the secret level. That network draws its information largely from the interagency Terrorist Threat Integration Center. The HSIN, also known as the Joint Regional Information Exchange system, is not yet connected to the Law Enforcement Online/Regional Information Sharing System/Open Source Information system network, which operates at the sensitive but unclassified level.
Source: http://www.gcn.com/vol1_no1/daily−updates/26420−1.html

[Return to top]

Emergency Services Sector

32. *June 30, Flint Journal (MI)* — **Anti−terror funds to shore up 911 system. The biggest part of more than $2 million Geneese county expects to receive to fight terrorism this year will help pay to plug the area into a statewide emergency dispatch system run by the Michigan state police.** The county Board of Commissioners gave initial approval to the spending plan Tuesday, rejecting Flint's appeal for more of the money. Only last month, officials who oversee the county's emergency dispatch system said they had cleared the last major hurdle for a new $10.3−million radio system to link local police and emergency workers to a statewide radio network. Part of that plan now involves using federal Homeland Security money to help local

police departments pay for radios compatible with with the new 800 MHz system. **The local planning team proposed the spending plan to county commissioners over the objections of Flint's representative, who had asked that money be set aside to create a city decontamination unit or for equipment for the police department's bomb squad.** Source: http://www.mlive.com/news/fljournal/index.ssf?/base/news−22/108860912045270.xml

33. *June 30, eWeek* — **Mississippi launches Linux−based safety system. The state of Mississippi has launched a Linux−based, mobile public safety system that links police, fire and emergency services to a single DB2 database.** Sen. Thad Cochran, R−MS, announced the successful initial deployment of the public safety system, Mississippi ASP (Automated System Project)—a mobile data infrastructure that's based on IBM eServer hardware and IBM DB2 and Novell SUSE Linux software, at a press conference at the University of Southern Mississippi. The Mississippi ASP's initial deployment links three Mississippi counties' law enforcement, fire department and emergency medical services to a DB2 database. When complete, the project will provide mobile units with real−time access to all available public safety information, including mug shots, arrest warrants, criminal intelligence, hazardous materials data and medical emergency protocols. "It is critical that all of our first responders have instant access to the critical information that can save lives, speed arrests and ensure public safety," Maj. Julian Allen, director of the ASP, said in a prepared statement.
Source: http://www.eweek.com/article2/0,1759,1618673,00.asp

34. *June 29, Department of Homeland Security* — **Internet course on America's new National Incident Management System. The Department of Homeland Security's Federal Emergency Management Agency (FEMA) announced on Tuesday, June 29, a new online course that will help first responders understand the concepts and principles underlying the new National Incident Management System (NIMS) and to begin incorporating NIMS into their own planning and policies.** "NIMS establishes standard incident management processes, protocols and procedures so that all responders − including those at the federal, state, tribal and local level − can coordinate their responses, share a common focus and place full emphasis on resolving the event," said Homeland Security Secretary Tom Ridge. "This new course introduces NIMS in a way that is easy and accessible to the nation's emergency responders." The training experts at Homeland Security's Emergency Management Institute created the online course, which takes about three hours to complete. The course can be found at: http://training.fema.gov/EMIWEB/IS/is700.asp
Source: http://www.dhs.gov/dhspublic/display?content=3799

[Return to top]

Information Technology and Telecommunications Sector

35. *July 01, Federal Computer Week* — **NIST aims to ease XP security setup.** Officials at the National Institute of Standards and Technology (NIST) hope their new publication will help simplify the process of setting security controls on Microsoft Corp.'s Windows XP Professional operating system. **NIST officials, who released the draft of Special Publication 800−68 this week, said the recommendations and security configuration checklists will help federal agencies fulfill their responsibilities for computer and information security under the**

Federal Information Security Management Act of 2002. The document's authors acknowledge the difficulty of setting reasonable security controls on an operating system as complex as Windows XP Pro. A publication that guides systems administrators and technical users through the process should help other federal agencies avoid time−consuming and costly mistakes, NIST officials said. They worked with the Defense Information Systems Agency, the National Security Agency, Microsoft and the nonprofit Center for Internet Security to reach a consensus on security settings for Windows XP and for productivity applications, e−mail, Web browsers, personal firewalls and antivirus programs that run on XP. Special Publication 800−68: http://csrc.nist.gov/itsec/guidance_WinXP.html
Source: http://www.fcw.com/fcw/articles/2004/0628/web−nist−06−29−04. asp

36. *July 01, Los Angeles Times* — **Beheading videos seen as new form of cyber−terrorism.** The slayings of businessman Nicholas Berg, engineer Paul M. Johnson Jr. and South Korean interpreter Kim Sun Il have been publicized through both conventional media channels and the Internet. **FBI Supervisory Special Agent Kenneth McGuire, who oversees the cyber−crime squad in Los Angeles, says that disseminating video of such violent acts over the Internet is a new form of cyber−terrorism −− one proving difficult to contain.** Publicizing their atrocities has always been part of the strategy for al Qaeda and other terrorist groups, says Josh Devon, an analyst at the SITE Institute in Washington, which tracks terrorist activities. **"The point of terrorism is to strike fear and cause havoc −− and that doesn't happen unless you have media to support that action and show it to as many people as they can**," Devon says. Terrorists used to circulate propaganda via publications and audio− or videotapes, but the Internet has supplanted those methods. In the United States, news executives who traditionally draw the line at depicting the most graphic war violence now face a media landscape where millions get unfiltered images on the Internet almost instantaneously. By posting digital video or photos on the Web, terrorist groups make it almost certain that the news media will air at least some of the images.
Source: http://news.yahoo.com/news?tmpl=story&u=/latimests/20040630/ts_latimes/webamplifiesmessageofprimitiveexecutions

37. *June 30, New York Times* — **Report calls for fixes in high−tech voting.** High−tech voting systems need quick fixes if they are to be used in the November election, according to a report released Tuesday, June 29, by a coalition of civil rights groups and computer security experts. The report, by the Brennan Center for Justice at New York University School of Law and the Leadership Conference on Civil Rights, lays out steps that state election officials should take in coming weeks to ensure that touch−screen voting machines perform as they should and merit voter confidence. **The recommendations include independent security review of machines and their software and procedures for monitoring election glitches**. The report concludes, "If implemented by those jurisdictions within the obvious constraints of time and resources, these recommendations can markedly improve confidence" that voting systems will function properly. **Electronic voting machines will be used by nearly a third of the nation's voters in November. But they have come under attack by computer security experts, who have found them vulnerable to tampering and mischief**. The report stopped short of demanding that states require that voting machines print a voter−verifiable receipt, which many experts have said will be necessary to provide the full measure of trust on high−tech voting but which would be almost impossible for states to put in place by November. Report: http://www.civilrights.org

Source: http://www.nytimes.com/2004/06/30/politics/campaign/30vote.h tml

38. *June 30, CNET News.com* — **Net service Ricochet bounces into new hands. Struggling Ricochet Networks, a pioneer among wireless Internet service providers, has been bought by YDI Wireless in a deal valued at $3.5 million.** Over the past several years, Ricochet has seen its ISP presence shrink to two markets, San Diego and Denver, from more than a dozen metropolitan areas. It's also undergone three ownership changes. YDI, a provider of wireless−infrastructure products, hopes to relaunch the service in New York, Los Angeles, San Francisco and the other major cities where the ISP used to operate. The company plans to retain the name "Ricochet" for the service.
Source: http://news.com.com/Net+service+Ricochet+bounces+into+new+ha nds/2100−1039_3−5253100.html?tag=nefd.hedd%20Telecommunicati ons

39. *June 30, Associated Press* — **In Hungary, creator of computer virus given suspended prison sentence.** A Hungarian court has convicted the teenage creator of a computer virus that infected tens of thousands of machines, sentencing the boy to two years probation, a newspaper reported Wednesday, June 30. The Veszprem City Court on Tuesday convicted the teenager, identified only as Laszlo K., for unauthorized use of computer systems. The virus spread through e−mail messages and was first noticed in May 2003. **The virus disabled the computer's anti−virus software, crippled the computer's mouse and printed messages disparaging the Microsoft Windows operating system.** Nepszabadsag reported that the teenager told the court he created the virus to prove to himself that he had some skills after failing several subjects at his high school in the town of Ajka, some 80 miles southwest of Budapest, the capital. **Police investigators tracked down the teenager with relative ease because he initially used his own e−mail address to send the infected messages.** The virus software also included most of the creator's name and the post code of his home.
Source: http://www.computerweekly.com/articles/article.asp?liArticle ID=131610

40. *June 30, InternetNews.com* — **Apache buffer overflow flaw patched.** The Apache Software Foundation has rolled out a patch for versions of its popular Apache HTTP Server to fix a potentially serious security flaw. **The buffer overflow flaw affects Apache httpd versions 1.3.26, 1.3.27, 1.3.28, 1.3.29 and 1.3.31, which were configured to act as proxy servers. Apache httpd 2.0 and other versions of Apache httpd 1.3 are unaffected.** An Apache Week advisory said the buffer overflow can be triggered by getting the mod_proxy feature to connect to a remote server and return an invalid content−length. The vulnerability is rated "important," but the advisory warned that **there is the possibility that it could be exploited to run arbitrary code.** "If you are running an Apache Web server, we'd recommend that you take a look at your configuration files and make sure that you have not inadvertently set up an open proxy. If you do not need your server to act as a proxy server, then make sure that the directive 'ProxyRequests On' does not appear in your configuration file," Apache said. The risk of code execution is high on older OpenBSD/FreeBSD distributions because of the internal implementation of memcpy, which re−reads the length value from the stack. On newer BSD distributions, it may be exploitable because the implementation of memcpy will write three arbitrary bytes to an attacker−controlled location, according to the alert. Linux and UNIX vendors, including Gentoo Linux, OpenBSD, Debian and Red Hat, have all issued updates to protect against the Apache Server bug.
Source: http://internetnews.com./security/article.php/3375521

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

Watch Synopsis: The Korgo virus is currently undergoing many variants in an effort to spread on the Internet. Part of the Korgo payload causes infected systems to download code from hacker−controlled websites. As these malicious websites are located and shut down by security personnel, new websites are created to host the malware. Ensure that your antivirus is up to date and check your logs for port 113 authentication requests to locate infected systems.

Current Port Attacks

Top 10 Target Ports	9898 (dabber), 445 (microsoft−ds), 135 (epmap), 5554 (sasser−ftp), 1434 (ms−sql−m), 137 (netbios−ns), 3127 (mydoom), 20168 (−−−), 1023 (Reserved), 4899 (radmin) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

41. *June 30, Associated Press* — **Statue of Liberty pedestal to reopen.** The 151−foot statue has been closed to the public since the September 11 attacks; however, the National Park Service has vowed to restore the public's ability to enter the statue's six−story pedestal this summer. **The event will be commemorated on Independence Day this Sunday, but the pedestal's reopening will not happen until late July or August**. And even then the inside of the 118−year−old statue will remain closed for security reasons. According to Brian Feeney, parks service spokesman, the problem is that the interior of the statue, which used to be accessible by a narrow spiral staircase, cannot be adequately secured. The pedestal, which contains the Statue of Liberty Museum, has had $7 million in improvements. They include improved lighting, a new fire suppression system and fire walls. There will be an additional staircase for exiting the pedestal and Fort Wood, the old stone fort on which the statue rests. The pedestal also will have an outdoor observation deck, where visitors will be able to walk around the statue's perimeter, and several undisclosed security measures, Feeney said.
Source: http://hosted.ap.org/dynamic/stories/S/STATUE_REOPENING?SITE=VTRUT&SECTION=HOME&TEMPLATE=DEFAULT

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP Web page (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Alerts − Advisories and Information Bulletins: DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues.

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports.

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer